The Applicants respectfully traverse these rejections based on the following points.

Sudia describes a multi-step digital signature method and system in which several signing devices participate, using a plurality of private signature key shares to affix a signature that can be verified using a single public verification key (see the Abstract). These signing devices are connected to several trusted devices of authorizing agents (col. 6, lines 43-50). The signing devices and trusted devices can be smart cards (col. 6, line 47, and col. 9, line 20).

In Sudia, each signing device and trusted device can store public/ private key pairs (i.e., encryption/decryption keys and signature/verification keys), wherein the public key of each key pair may be certified by a certification authority. Therefore, each signing device and trusted device can store public key certificates to provide assurance to the public that a public key identified in a certificate is issued by the device whose identification number is in the certificate (col. 1, lines 19-24). These certificates can be signed using Sudia's multi-step method and system (col. 2, lines 25-30).

As Sudia describes in column 8, lines 35-41, and in column 9, lines 45-49, the certificates can also be generated and signed by a manufacturer and then included in a trusted or signing

device. These certificates contain the device's serial number and a public key, along with the device's model number and other trusted characteristics.

In Sudia, the certificates can also be generated by a temporary administrator. Upon reception of a certification request from a signing or trusted device, an administrator (which is not a PSD) signs with its own private signature key a certificate that comprises the name of the requesting signing device and a public signature verification key generated by the requesting signing device (see col. 10, line 45, through col. 11, line 20, and col. 11, line 53, through col. 12, line 14).

In Sudia, during a re-certification process, the certificates can also be signed using a multi-step method. Upon reception of a certification request from a signing or trusted device, a plurality of signing devices sign, with their own private signature key shares, a certificate that comprises the name of the requesting signing device and a public signature verification key generated by the requesting signing device (see col. 13, line 53, through col. 14, line 53, and col. 15, line 13, through col. 16, line 3).

As a conclusion, in all the certificate generation methods described in Sudia, a complete certificate is not generated by the requesting signing or trusted device, which generates the

public key to be certified. This certificate has to be signed by an authority (manufacturer, temporary administrator, or multiple other signing devices) using a private key of that authority and not a key generated by the requesting signing or trusted device.

In particular, the inventions defined by independent claims 1, 26, 30 and 32 are differentiated from the teachings of Sudia at least in that the claimed invention provides for a certificate generating system, which uses a key generated by the requesting signing or trusted device. Sudia lacks any teaching of a complete certificate generated by the requesting signing or trusted device which generates the public key to be certified, but instead the certificate of Sudia has to be signed by an authority (manufacturer, temporary administrator, or multiple other signing devices) using a private key of that authority.

Moreover, the certificate validating inventions of claims 13, 27, 31 and 33 are distinguished from Sudia as follows. Validating a certificate generated by use of one of the methods described in Sudia involves the use, by the verifying system of the public verification key, of the authority that signed the certificate. Therefore, it may need cross-referencing means for selecting the proper public verification key (and eventually a proper public decryption key) by use of an identifier of the authority. But the system of Sudia does not involve

cross-referencing a unique device name of a PSD contained in the certificate with at least one proper cryptographic key and with one proper cryptography algorithm in order to extract useful information from the certificate. The features of independent claims 13, 27, 31 and 33 concerning these cross-referencing aspects differentiate the claimed invention from Sudia.

Accordingly, the Applicants respectfully submit that Sudia does not anticipate the subject matter defined by independent claims 13, 26, 27, and 30-33. Therefore, allowance of claims 13, 26, 27, and 30-33 and all claims dependent therefrom is warranted.

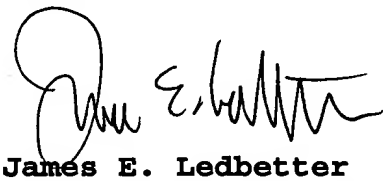
Turning now to the rejections of claims 1-12 based on Sudia and Schell, the Applicants reiterate that Sudia lacks any teaching or suggestion of a system for generating a certificate by a PSD whose identifier is contained in the certificate, in dependence of a key generated by the PSD. Further, although Schell describes a data processing system and method for generating or validating a key protection certificate, Schell's certificate has to be signed by a certification authority to be valid. Such a certificate is not generated by a PSD whose identifier is contained in the certificate, in dependence on a key generated by the PSD, as required by claim 1.

Accordingly, the Applicants respectfully submit that Schell fails to cure the above-noted deficiencies of Sudia and that Sudia and Schell, considered alone or together, do not disclose or suggest the subject matter defined by claim 1. Therefore, allowance of claim 1 and claims 2-12 dependent therefrom is warranted.

In view of the above, it is submitted that this application is in condition for allowance and a notice to that effect is respectfully solicited.

If any issues remain which may best be resolved through a telephone communication, the Examiner is requested to telephone the undersigned at the local Washington, D.C. telephone number listed below.

Respectfully submitted,



Date: August 26, 2005
JEL/DWW/att

James E. Ledbetter
Registration No. 28,732

Attorney Docket No. L741.01105
STEVENS DAVIS, MILLER & MOSHER, L.L.P.
1615 L Street, N.W., Suite 850
P.O. Box 34387
Washington, D.C. 20043-4387
Telephone: (202) 785-0100
Facsimile: (202) 408-5200